CLAIMS

What is claimed is:

1. A security system for use in conjunction with data flowing from a first device to a second device being directed to said second device in accordance with a network address of said second device, said system comprising:

a security device connected between said first and second devices, said security device accepting packet data for bridging to said second device, said security device operable for observing data flowing from said first device to said second device, said security device not itself having a network address.

2. The security system of claim 1 wherein said first device could be any device on the unsecured side of said security device, each said first device having a unique network address, and wherein said second device could be any device on the secured side of said security device, each said second device having a unique network address.

3. The security system of claim 2 wherein said security device maintains a list of addresses for which it has security responsibility and wherein said security device only observes those data packets containing the network addresses maintained in said list.

4. The security system of claim 3 wherein said list includes addresses of both said first devices and said second devices.

5. The security system of claim 1 wherein said observing comprises:

a monitoring system for gathering information pertaining to the operation of said second device; and

a mechanism for modifying the flow of data into said security system depending upon said gathered information.

6. The security system of claim 5 wherein said gathered information is selected from the list containing:

number of arriving packets in a particular time interval;

the type of requests contained within given packets;

the nature of the informational content of the packets;

the sending identity of the packets;

the destination of the packets;

the traffic patterns formed by packets from specific sources;

the number of arriving packets from specific sources;

the correctness of the packets;

certain data contained in one or more messages; and

the type of file attached to a message.

7. The security system of claim 5 wherein said flow modifying mechanism operates to compare said gathered information with certain pre-established criteria and to set limits, and wherein said operational characteristics of said mechanism is modified in accordance with said set limits.

8. A security device for use in a packet data network where packets are delivered from a sending location to a destination location based upon one or more destination network addresses associated with each packet, said security device comprising:

at least one NIC card for receiving data packets;

a database for maintaining a list of destination network addresses to be secured by said device; and

wherein said at least one NIC card is connected to said network at any point between a sending location and one or more destination locations, said NIC card maintained in promiscuous mode such that said security device can observe all data directed to any destination addresses maintained from time to time in said list.

9. The security device of claim 8 wherein said security device is connected to said network without establishing a network address for said security device.

10. The security device of claim 9 wherein said security device can be moved from location to location on said network without changing any network settings.

11. The security device of claim 8 further comprising:

a plurality of NIC cards all operating in said promiscuous mode.

12. The security device of claim 11 wherein said security device has a zero network footprint while said NIC cards are in said promiscuous mode.

13. The security device of claim 12 wherein all of said NIC cards share the same destination list.

14. The security device of claim 8 wherein said observing comprises:

monitoring system for gathering information pertaining to the operation of said second device; and

mechanism for modifying the flow of data into said security system depending upon said gathered information.

15. The security device of claim 14 number of arriving packets in a particular time interval;

the type of requests contained within given packets;

the nature of the informational content of the packets;

the sending identity of the packets;

the response destination of the packets;

the traffic patterns formed by packets from specific sources;

the number of arriving packets from specific sources;

certain data contained in one or more messages; and

the type of file attached to a message.

16. The security device of claim 15 wherein said flow modifying mechanism operates to compare said gathered information with certain pre-established criteria and to set limits, and wherein said operational characteristics of said gateway router are modified in accordance with said set limits.

17. A method for monitoring data packets arriving at a destination device, said data packets including a network address said packets traveling on a network defined in accordance with said network addresses, said method comprising the steps of:

inserting a security device into said network at a particular location between a sending device and a destination device; and

establishing within said security device the network addresses of said destination device.

18. The method of claim 17 wherein said destination device is a plurality of devices and wherein said establishing step comprises:

establishing all of said plurality of destination devices within said security device.

19. The method of claim 18 wherein at least one of said destination devices is on a public side of said security device so as to monitor data packets egressing from a private side of security device.

20. The method of claim 17 further comprising the step of:

setting said security device to operate in the promiscuous mode.

21. The method of claim 20 further comprising the step of:

modifying the delivery of data to said destination based upon the content of information in arriving data packets.

22. The method of claim 17 wherein said security device does not have a network location address.

23. The method of claim 22 further comprising the steps of:

blocking certain data packets from reaching said destination device;

blocking all packets from reaching said destination device;

load balancing between devices;

modifying the informational content of certain ones of said packets;

unblocking certain hitherto blocked packets, on the basis of certain parameters; and

modifying the informational content of certain ones of said packets.

24. The method of claim 17 further comprising the steps of:

monitoring data packets leaving said destination device; and

selectively modifying the operational characteristics of any network traveled by said data packets based upon the content of said leaving packets.

25. The method of claim 17 wherein said inserting step can be accomplished without changing network configuration settings.

26. The method of claim 17 wherein said inserting step can be performed while said network is operating.

27. The method of claim 17 further comprising the step of:

removing said security device form said particular location while said network is operating.

28. A security device for connection in a data network ahead of a plurality of data destinations to be protected, each said destination identifiable by a unique network address, said security device comprising:

means for accepting data packets from said network without said data packets being addressed to said security device; and

means for passing accepted data packets to particular ones of said data destinations in accordance with destination addresses of said destinations to be detected and maintained for said security device.

29. The security device of claim 28 wherein said maintained destination addresses are stored in a database internal to said security device.

30. The security device of claim 28 wherein said accepting means comprises:

at least one network termination operating in a promiscuous mode.

31. A method of operating a security device connected to a data network ahead of a plurality of data destinations to be protected, each said destination identifiable by a unique network address, said data network having a plurality of nodes, said method comprising the steps of:

accepting data packets from said network without said data packets being addressed to said security device; and

passing accepted data packets to particular ones of said data destinations in accordance with destination addresses of said destinations to be detected and maintained for said security device.

32. The method of claim 31 further comprising:

real time review of certain parameters pertaining to data flowing between nodes of said network;

means for comparing said monitored parameters against stored criteria; and

means for feeding data traffic affecting signals to one or more of said nodes under at least partial control of said comparing means.

33. The method of claim 32 wherein said stored criteria are dynamically changeable.

34. The method of claim 32 further including the step of:

storing certain of said monitored parameters for a period of time, at least some of said stored parameters being useful in determining at least a portion of the communication history of said monitored data.

35. The method of invention claim 32 wherein at least one of said nodes to which data traffic attaches signals is a gateway node to said destination to be protected.